Title (en)

SECRET AGGREGATE FUNCTION CALCULATION SYSTEM, SECRET CALCULATION DEVICE, SECRET AGGREGATE FUNCTION CALCULATION METHOD, AND PROGRAM

Title (de)

SYSTEM ZU BERECHNUNG EINER GEHEIMEN SUMMENFUNKTION, VERFAHREN ZU BERECHNUNG EINER GEHEIMEN SUMMENFUNKTION UND PROGRAMM ZUR BERECHNUNG EINER GEHEIMEN SUMMENFUNKTION

Title (fr)

SYSTÈME DE CALCUL DE FONCTION AGRÉGÉE DE SECRET, DISPOSITIF DE CALCUL DE SECRET, PROCÉDÉ DE CALCUL DE FONCTION AGRÉGÉE DE SECRET, ET PROGRAMME

Publication

EP 3806070 A4 20220126 (EN)

Application

EP 19806536 A 20190514

Priority

- JP 2018100626 A 20180525
- JP 2019019093 W 20190514

Abstract (en)

[origin: EP3806070A1] To efficiently determine intermediate data for use with an aggregate function while keeping confidentiality. A bit decomposition unit (11) generates a share of a bit string by bit decomposition and concatenation of key attributes. A group sort generation unit (12) generates a share of a first permutation, which performs a stable sort of the bit string in ascending order. A bit string sorting unit (13) generates a share of a sorted bit string obtained by sorting the bit string with the first permutation. A flag generation unit (14) generates a share of a flag indicating a boundary between groups. A key aggregate sort generation unit (15) generates a share of a second permutation, which performs a stable sort of the negation of the flag in ascending order. A de-duplication unit (16) generates shares of de-duplicated key attributes. A key sorting unit (17) generates shares of sorted key attributes by sorting the de-duplicated key attributes with the first permutation and the second permutation in sequence. A value sorting unit (18) generates shares of the sorted value attributes by sorting value attributes with the first permutation.

IPC 8 full level

H04L 9/08 (2006.01); **G06F 16/242** (2019.01); **G09C 1/00** (2006.01)

CPC (source: EP US)

G06F 16/244 (2019.01 - EP US); **H04L 9/085** (2013.01 - EP US); H04L 2209/46 (2013.01 - EP US)

Citation (search report)

- [Y] EP 3096308 A1 20161123 - NIPPON TELEGRAPH & TELEPHONE [JP]
- [Y] KOKI HAMADA ET AL: "An Algorithm for Computing Aggregate Median on Secure Function Evaluation", COMPUTER SECURITY SYMPOSIUM 2012, 23 October 2012 (2012-10-23), http://id.nii.ac.jp/1001/00086688/, pages 509 - 516, XP055507586
- [Y] LAUD PEETER: "Parallel Oblivious Array Access for Secure Multiparty Computation and Privacy-Preserving Minimum Spanning Trees", PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES, 1 June 2015 (2015-06-01), pages 188 - 205, XP055872908, Retrieved from the Internet <URL:https://petsymposium.org/2015/papers/10_Laud.pdf> [retrieved on 20211214], DOI: 10.1515/popets-2015-0011
- [YD] DAI IKARASHI ET AL: "A Design and an Implementation of Super-high-speed Multi-party Sorting: The Day When Multi-party Computation Reaches Scripting Languages", PROCEEDINGS OF COMPUTER SECURITY SYMPOSIUM 2017, vol. 2017, no. 2, 1 January 2017 (2017-01-01), pages 600 - 607, XP055593400
- See also references of WO 2019225401A1

Cited by

US11593114B1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

EP 3806070 A1 20210414; **EP 3806070 A4 20220126**; **EP 3806070 B1 20230719**; AU 2019273208 A1 20201210; AU 2019273208 B2 20210916; CN 112119442 A 20201222; CN 112119442 B 20240712; JP 6989006 B2 20220105; JP WO2019225401 A1 20210527; US 11593362 B2 20230228; US 2021191927 A1 20210624; WO 2019225401 A1 20191128

DOCDB simple family (application)

EP 19806536 A 20190514; AU 2019273208 A 20190514; CN 201980032660 A 20190514; JP 2019019093 W 20190514; JP 2020521167 A 20190514; US 201917057120 A 20190514